vereinswelt
Damit Vereinsführung Freude macht!

Datenschutzrecht 2018

Was bedeutet das?
8 wesentliche Datenschutzrechte
So bereiten Sie Ihren Verein vor

So bereiten Sie Ihren Verein auf das neue Datenschutzrecht ab 2018 vor von Heiko Klage

„Alles neu macht der Mai.“ Gemeint ist der Mai 2018, genauer der 25. Mai 2018. Ab diesem Datum werden europaweit die Weichen im Datenschutzrecht neu gestellt. Denn dann tritt die EU-Datenschutzgrundverordnung (DSGVO) in ganz Europa unmittelbar in Kraft. Sie gilt dann sofort auch für Vereine verbindlich. Mit gleichem Datum wird das bisherige deutsche Bundesdatenschutzgesetz (BDSG) geändert. Zukünftig ergänzt es nur noch die DSGVO. Die Anzahl der auch von Vereinen zu beachtenden Vorschriften vervierfacht sich damit mal eben. Deshalb: Nutzen Sie die verbleibende Zeit. Verschaffen Sie sich einen Überblick über die wichtigsten kommenden Regelungen. Erfahren Sie hier, was Sie jetzt schon vorbereiten können

Das bedeutet die Datenschutzgrundverordnung

Mehr Kontrolle für Verbraucher: Bisher war der Standard im Datenschutzrecht europaweit sehr unterschiedlich. Das soll angeglichen werden. Eine der Kernideen dabei ist, dass Verbraucher mehr Kontrolle über ihre Daten bekommen sollen. Die EU-Datenschutzgrundverordnung (DSGVO) bringt daher einige Neuerungen zur Erfassung, Aufbewahrung und Verwendung von persönlichen Daten mit sich.

Die DSGVO hat Auswirkungen auf die EDV-Prozesse und auf viele andere Bereiche in Ihrem Verein, zum Beispiel auch auf die Bereiche Mitgliederwerbung und Meldung an Dachverbände. Es müssen sämtliche Prozesse, die in irgendeiner Form Kontakt mit persönlichen Daten auslösen, auf den Prüfstand.

HoheBußgelder und Abmahnungen drohen: Deutlich teurer werden mit der neuen DSGVO die Bußgelder bei Datenschutzverstößen. Die Obergrenze für Bußgelder liegt bei sage und schreibe 20 Millionen Euro oder ggf. bei vier Prozent des Weltjahresumsatzes des Vorjahres. Nun brauchen Sie natürlich nicht damit rechnen, dass gegen ihren Verein derart hohe Bußgelder festgesetzt werden. Teurer wird es aber alle Mal. Im vierstelligen Bereich dürften sich die Strafen auf jeden Fall bewegen.

Rechnen Sie auch damit, dass nach dem 25. Mai 2018 Verbraucherschützer und konkurrierende Vereine kostenpflichtige Abmahnungen aussprechen, wenn Ihr Verein die datenschutzrechtlichen Vorgaben nicht umsetzt. Erfahrungsgemäß beginnt dieser Abmahnungsirrsinn immer sehr schnell nach dem Inkrafttreten entsprechender gesetzlicher Änderungen, also Ende Mai 2018.

Die 8 wesentlichen Datenschutzrechte Ihrer Mitglieder im Überblick

Schutz persönlicher Daten: Die DSGVO ist nicht in Paragrafen, sondern in 99 Artikel gegliedert. Ihnen sind 173 Erwägungsgründe vorangestellt, in denen das EU-Parlament seine Absichten und Ziele bei der DSGVO darstellt und die Regelungen aus den einzelnen Artikeln konkretisiert. Auch nach dem neuen Datenschutzrecht geht es um den Schutz persönlicher Daten wie Name, Adresse, Geburtsdatum, Kontoverbindung, ggf. Gesundheitsinformationen usw.

8 wesentliche Rechte: Ihre Mitglieder, die Interessenten für eine Mitgliedschaft und die Mitarbeiter Ihres Vereins haben aufgrund der DSGVO acht wesentliche Rechte im Hinblick auf den Datenschutz.

8 wesentliche Rechte und was das für Ihren Verein bedeutet

Das Recht auf Zugang zu Informationen

Das bedeutet für Ihren Verein: Alle Personen haben das Recht, auf ihre eigenen personenbezogenen Daten zuzugreifen. Weiter haben sie einen Anspruch darauf, zu erfahren, wie Sie diese Daten verwenden. Auf Wunsch muss Ihr Verein eine Kopie der personenbezogenen Daten kostenlos elektronisch zur Verfügung stellen.

Das Recht auf Vergessen werden

Das bedeutet für Ihren Verein: Mitglieder haben einen Anspruch darauf, vergessen zu werden. Das gilt insbesondere beim Ende der Mitgliedschaft oder wenn Ihrem Verein die weitere Nutzung der Daten untersagt wird. Das bedeutet auch, dass Sie Dritte, an die Sie die Daten übermittelt haben, informieren müssen, wenn Sie unrichtige Daten berichtigt haben, bestrittene Daten gesperrt haben, unzulässig erhobene Daten gesperrt haben.

Hiervon betroffen sind etwa Daten, die Sie an Dachverbände weitergegeben haben. Ihre (Ex-)Mitglieder haben den Anspruch auf Information von Dachverbänden usw. nicht, wenn die Information einen unverhältnismäßig hohen Aufwand erfordert und schutzwürdige Interessen der unterlassenen Information nicht entgegenstehen

Das Recht auf Portabilität der Daten

Das bedeutet für Ihren Verein: Insbesondere bei Service-Anbietern wird die Übertragbarkeit von Daten wichtig. Betroffene haben einen entsprechenden Anspruch auf Übertragung der Daten in einem üblichen maschinenlesbaren Format. Beachten Sie dabei aber folgende Kontrollfragen:

Wie stellen Sie sicher, dass der Übertragungswunsch von einer berechtigten Person, also wirklich Ihrem Mitglied, stammt? Sind die zu übertragenen Daten wirklich beim Mitglied legal erhoben? Wie erfolgt die Datenübertragung praktisch (nach Wahl des Mitglieds in elektronischer Form an ihn oder einen anderen Verantwortlichen, Art. 20 DSGVO)?

Das Recht auf Information und Freigabe

Das bedeutet für Ihren Verein: Bevor Ihr Verein Daten sammelt, müssen Sie die Betroffenen darüber informieren. Diese müssen der Erfassung der Daten in der Regel ausdrücklich zustimmen. Ein stillschweigendes Einverständnis reicht nicht. Das heißt: Alle Prozesse, mit denen Ihr Verein Daten sammelt, müssen daraufhin überprüft und angepasst werden. Es muss sichergestellt sein, dass das eingeholte Einverständnis dokumentiert und gespeichert wird.

Das Recht auf Berichtigung falscher Daten

Das bedeutet für Ihren Verein: Wie bisher gibt es einen Berichtigungsanspruch, wenn Daten veraltet, unvollständig oder falsch sind

Das Recht auf Einschränkung der Datennutzung

Das bedeutet für Ihren Verein: Einzelpersonen dürfen verlangen, dass ihre persönlichen Daten nicht weiterverarbeitet werden. Sie dürfen diese dann zwar weiter speichern, im Ergebnis aber nicht verwenden.

Das Einspruchsrecht

Hintergrund sind die Methoden im Direktmarketing. Direktmarketing wird von vielen als besonders störend empfunden. Deshalb dürfen Einzelpersonen Einspruch gegen die Verwendung ihrer Daten für direktes Marketing einlegen. Hierüber müssen Sie bei der Erhebung der Daten informieren. Sobald die Betroffenen Einspruch eingelegt haben, dürfen die Daten nicht mehr verwendet werden.

Der Anspruch auf Benachrichtigung

Kommt es zu einem Problem mit der Datensicherheit, das personenbezogene Daten betrifft (z. B. Klau von Kreditkartendaten), muss Ihr Verein die Betroffenen in der Regel innerhalb von 72 Stunden informieren. Das bedeutet, dass:
Ihr Verein im eigenen Interesse die Datensicherheit optimieren muss.
Ihr Verein Maßnahmen einrichten muss, damit Probleme bei der Datensicherheit erkannt werden
Einen Prozess definieren muss, um im Falle eines Falles innerhalb von 72 Stunden zu informieren.

Nach wie vor: Datenverarbeitung ist grundsätzlich verboten

Auch unter dem bisherigen Datenschutzrecht galt, dass die Datenverarbeitung grundsätzlich verboten ist. Sie ist nur erlaubt, wenn es dafür entweder eine gesetzliche Grundlage gibt oder aber Mitglieder und Interessenten ausdrücklich eingewilligt haben. Geregelt ist das Ganze in Artikel 6 DSGVO, der insgesamt sechs Erlaubnistatbestände vorsieht:

Übersicht: 6 Gründe für die Zulässigkeit der Datenverarbeitung gemäß Art 6 Abs. 1 Satz 1 DSGVO

	Für Vereine besonders relevant?
Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben.	Ja
Die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen	Ja
Die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verein unterliegt.	Ja
Die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen.	
Die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die Ihrem Verein übertragen wurde.	
Die Verarbeitung ist zur Wahrung der berechtigten Interessen Ihres Vereins oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.	Ja

Das bedeuten die Erlaubnisgründe im Einzelnen

Erforderlichkeit zur Abwicklung eines Vertrags (Art. 6 Abs. 1 Satz 1b DSGVO)

Mitgliederdaten, die Sie benötigen, um die Erfüllung eines Vertrags sicherzustellen, dürfen Sie ohne ausdrückliche Einwilligung des Vertragspartners verarbeiten (Art. 6 Abs. 1 Satz 1b DSGVO).

Auch das Mitgliedsverhältnis zwischen Mitglied und Verein ist davon umfasst. Das Gleiche gilt für Daten, die Ihnen jemand übermittelt hat, der Interesse an der Mitgliedschaft in Ihrem Verein hat.

Ähnlich wie im bisher geltenden Recht gilt das aber nur für die zur Vertragserfüllung erforderlichen Daten, nicht für Daten, die Sie eventuell für spätere Zwecke für sinnvoll halten. Sofern Sie Daten erheben und verarbeiten wollen, die für die Erfüllung nicht erforderlich sind, benötigen Sie dazu die Einwilligung des Vertragspartners.

Erforderliche Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung, der ihr Verein unterliegt (Art. 6 Abs. 1 Satz 1c DSGVO)

Eine ähnliche ausdrückliche Regelung gab es bisher nicht. Mit „rechtliche Verpflichtung“ sind gesetzliche Normen gemeint, die sich aus EU-Recht oder aus dem deutschen Recht ergeben.

Nicht gemeint sind etwa Satzungen von Dachverbänden, denen Ihr Verein angehört. Diese Regelung erlaubt Ihnen, zum Beispiel die Speicherung von Daten, soweit dies für die Erfüllung gesetzlicher Aufbewahrungspflichten erforderlich ist.

Datenverarbeitung ist zur Wahrung der berechtigten Interessen Ihres Vereins oder eines Dritten erforderlich (Art. 6 Abs. 1 Satz 1f DSGVO)

Wenn die konkrete Datenverarbeitung zur Wahrung der berechtigten Interessen Ihres Vereins oder eines Dritten erforderlich ist, ist sie nach dieser Vorgabe erlaubt. Voraussetzung ist allerdings, dass nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Datenschützer rechnen schon jetzt damit, dass es um diese Regelung eine Vielzahl von Auseinandersetzungen geben wird. Denn die Frage, wann ein ausreichendes berechtigtes Interesse vorliegt und wann möglicherweise entgegenstehende Interessen oder Grundrechte der Betroffenen überwiegen, lässt im Einzelfall viel Interpretationsspielraum zu.

Das Risiko dabei ist, dass Sie in jedem Einzelfall entscheiden müssen, ob die Voraussetzungen vorliegen. Legen Sie mit Ihrer Einschätzung falsch, liegt ein Datenschutzverstoß vor, der die erwähnten Bußgelder auslösen kann. Daher sollten Sie folgende Aspekte des Art. 6 Abs. 1 Satz 1 f. DSGVO berücksichtigen:

Wichtige Einschränkungen:

1. Grundsätzlich reichen berechtigte Interessen für die Datenverarbeitung aus. Sie müssen aber zwei Einschränkungen beachten:
   ➔ Die konkrete Datenverarbeitung muss für die verfolgten berechtigten Interessen erforderlich sein (= deutlich mehr als „nützlich“ sein).
   ➔ Die Regelung hilft nicht, wenn die schutzwürdigen Interessen des Betroffenen überwiegen.

2. Bei der Frage, ob berechtigte Interessen vorliegen, sind auch die Grundsätze des Datenschutzes zu berücksichtigen. Dazu gehören unter anderem der Grundsatz der Datensparsamkeit und der Grundsatz der Datenrichtigkeit. So kann zum Beispiel ein berechtigtes Interesse an der Verarbeitung des Geburtsdatums bestehen, um zu vermeiden, dass mehrere Personen mit gleichem Namen in der Datenbank verwechselt werden.

3. Ein berechtigtes Interesse besteht nicht, wenn vernünftige Erwartungen der Betroffenen entgegenstehen (Erwägungsgrund 47 DSGVO). Solche vernünftigen Erwartungen können zum Beispiel vorliegen, wenn der Betroffene mit der (weiteren oder anhaltenden) Datenverarbeitung nicht rechnen musste, weil etwa das Mitgliedsverhältnis beendet ist.

Wichtig: Besonderes Widerspruchsrecht

Ausdrücklich für die Datenverarbeitung aus berechtigtem Interesse gibt es ein besonderes Widerspruchsrecht in Art. 21 DSGVO. Aus Gründen, die sich aus der besonderen Situation ergeben, haben Betroffene jederzeit das Recht, Widerspruch gegen die Verarbeitung sie betreffender personenbezogener Daten einzulegen. Ihr Verein muss dann die Verarbeitung dieser Daten sofort einstellen.

„Besondere Situation“ bedeutet, dass der Betroffene auch mündlich Gründe darlegen kann, die ihm – anders als anderen Personen – die Verarbeitung von Daten über seine Person unzumutbar macht. Der Wunsch, generell nicht in Datenbanken und Ähnlichem erfasst zu sein, reicht dafür aber nicht.

Das Widerspruchsrecht besteht nicht, wenn Sie zwingende schutzwürdige Gründe für die Datenverarbeitung nachweisen können, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen. Was die Gerichte und Aufsichtsbehörden darunter konkret verstehen werden, bleibt abzuwarten. Eine weitere Ausnahme gilt, wenn die Datenverarbeitung der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen durch Ihren Verein dient.

Beispiel: *Ihr Mitglied hatte sich zu einer Vereinsreise angemeldet. Allerdings ist es zum Streit darüber gekommen, ob Ihr Mitglied diese Reise schon in vollem Umfang bezahlt hat. Die Daten aus seiner Anmeldung, seiner Teilnahme und der Bezahlung inklusive der Kontonummern dürfen Sie dann speichern.*

Widerspruch per Mausklick

Art. 21 DSGVO schreibt weiter vor, dass der Widerspruch mittels automatisierter Verfahren ausgeübt werden kann, bei denen technische Spezifikationen verwendet werden. Im Klartext ist gemeint, dass ein „Widerspruch per Mausklick“ möglich sein soll.

Spätestens bei der ersten Kommunikation mit dem Betroffenen müssen Sie ihn ausdrücklich auf dieses Widerspruchsrecht hinweisen. Dies muss einerseits verständlich und andererseits von anderen Informationen getrennt erfolgen, zum Beispiel so:

Sie können jederzeit aus Gründen, die sich aus ihrer besonderen Situation ergeben, Widerspruch gegen die Verarbeitung ihrer personenbezogenen Daten bei uns einlegen. Den Widerspruch können Sie beispielsweise auf folgender Webseite …(Link) einlegen.

Sobald der Widerspruch bei Ihnen eingeht, sind Sie verpflichtet, den entsprechenden Datensatz zu sperren, bis Sie überprüft haben, ob eine der oben angesprochenen Ausnahmen greift, die Sie zur Weiterverarbeitung der Daten berechtigt. Liegt eine solche Ausnahme nicht vor, müssen Sie den Datensatz nach Ende Ihrer Prüfung löschen. Die Prüfung müssen Sie unverzüglich vornehmen, spätestens innerhalb eines Monats. Ist das ausnahmsweise nicht möglich, müssen Sie dem Betroffenen die Gründe für die Verzögerung mitteilen. Dann kann die Frist auf bis zu drei Monate verlängert werden (Art. 12 DSGVO).

Das müssen Sie zur Einwilligung in die Datenverarbeitung wissen

Sofern nicht ausnahmsweise einer der anderen Erlaubnisgründe des Art. 6 Abs. 1 vorliegt (siehe oben), ist die ausdrückliche Einwilligung des Mitglieds in die Datenverarbeitung erforderlich. Dazu gehört auch, dass Sie Ihre Mitglieder darüber informieren, wofür Sie diese Daten einsetzen werden.

Verbesserungendurch die DSGVO

Das neue Datenschutzrecht bringt nicht nur Verschlechterungen mit sich. Bisher war für die Einwilligung in die Datenschutzvereinbarung grundsätzlich die Schriftform vorgeschrieben (§ 4a BDSG). Die elektronische Form war unter engen Voraussetzungen zulässig (§ 13 Telemediengesetz). Ähnliches galt bisher für die elektronische Einwilligung für Adresshandel und Werbung (§ 28 Absatz 3a BDSG).

So kann die Einwilligung erfolgen

Erlaubt sind zukünftig folgende Formen der Einwilligung:

- ➔ Schriftliche Einwilligung,
- ➔ Einwilligung durch aktives Betätigen einer Checkbox,
- ➔ Einwilligung per E-Mail, mündliche Einwilligung (aber nicht zu empfehlen, da nicht beweisbar),
- ➔ Einwilligung durch entsprechende Voreinstellungen im Browser.

Die Zustimmung muss aber eindeutig erklärt werden. Eine konkludente Zustimmung durch schlüssiges Verhalten (z. B. bloße Bestellung eines Newsletters ohne ausdrückliche Zustimmung zur Speicherung und Verarbeitung der Daten) reicht nur, wenn sie „eindeutig bestätigenden Charakter“ hat. Setzen Sie daher am besten auf ausdrückliche Erklärungen.

Die DSGVO schreibt weiter vor, dass eine Einwilligung nur gültig ist, wenn sie freiwillig und in informierter Weise erfolgt. Den Betroffenen muss also klar sein, welche Daten zu welchem konkreten Zweck wie genutzt werden. Sie müssen sie also über Folgendes informiert sein:

Informationen an Mitglieder

- ➔ Um welche Daten geht es?
- ➔ Zu welchem Zweck werden sie verarbeitet?
- ➔ Wie werden die Daten genutzt?
- ➔ Wer ist die verarbeitende Stelle? (= Ihr Verein)

Einwilligung per Checkbox Eine sogenannte Opt-out-Lösung ist unzulässig. Opt-out bedeutet, dass die Zustimmung zur Datenspeicherung etwa bei einem Bestellformular im Internet als Vorauswahl eingestellt ist. Der Kunde muss diese Vorauswahl aktiv löschen, wenn er mit der Datenspeicherung nicht einverstanden ist.

Erforderlich ist hingegen eine sogenannte Opt-in Lösung, bei der der Ihr Mitglied zum Zeichen seines Einverständnisses aktiv einen Haken setzen muss.

> ❑ *Ich bin damit einverstanden, dass das Unternehmen XY meinen Namen und meine E-Mail-Adresse zum Zweck des Versands des monatlichen Kunden-Newsletters speichert und verwendet. Dieses Einverständnis kann ich jederzeit widerrufen, ohne dass mir dafür andere Kosten als die für die Datenübertragung nach dem Grundtarif entstehen.*

Am besten gestalten Sie eine sogenannte Double Opt-in Lösung. Das kennen Sie bereits. Nachdem der Kunde die Checkbox aktiviert hat, erhält er eine automatisierte E-Mail, mit der Aufforderung, seine Registrierung per Klick auf einen in der E-Mail angegebenen Link zu aktivieren. Damit soll verhindert werden, dass Unberechtigte im fremden Namen Bestellungen aufgeben, Registrierungen vornehmen usw.

Für verschiedene Vorgänge müssen Sie jeweils separate Zustimmungen einholen und nachweisen können.

Es spricht jedoch nichts dagegen, das Einverständnis mit mehreren Verarbeitungszwecken in einem Dokument zusammenzufassen (Erwägungsgrund 32 Satz 4 und 5 DSGVO). Damit reduzieren Sie den Verwaltungs- und Dokumentationsaufwand in Ihrem Verein erheblich.

Diese Rechte haben Betroffene

Neben dem bereits angesprochenen Widerspruchsrecht aus berechtigtem Interesse bringt die Verordnung einige weitere Änderungen bei den Betroffenenrechten mit sich. Dazu gehören:

- ➔ Eine Erweiterung der Auskunftspflicht,
- ➔ ein neues Zugriffsrecht,
- ➔ eine Berichtigungspflicht und
- ➔ ein Recht auf Löschung.

Erweiterung der Auskunftspflicht

Artikel 15 DSGV erweitert die Auskunftspflichten, denen sich Ihr Verein stellen muss. Betroffene sind berechtigt, Auskunft darüber zu verlangen, ob Sie personenbezogene Daten über sie verarbeiten. Wenn ja, besteht weiter ein Recht auf Auskunft über diese personenbezogenen Daten und auf folgende weitere Informationen:

- ➔ Verarbeitungszwecke,
- ➔ Kategorien personenbezogener Daten, die verarbeitet werden,
- ➔ Empfänger oder Kategorien von Empfängern gegenüber denen die Daten offengelegt wurden oder noch offengelegt werden,
- ➔ falls möglich, die geplante Dauer für die die Daten gespeichert werden, andernfalls die Kriterien für die Festigung dieser Dauer,
- ➔ das Bestehen eines Rechts auf Berichtigung oder Löschung der Daten oder auf Einschränkung der Verarbeitung,
- ➔ das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde,
- ➔ sofern die Daten nicht bei dem Betroffenen selbst erhoben wurden, alle verfügbaren Informationen über die Herkunft der Daten (z. B. Angabe des Adresshändlers, wenn Sie Adressdaten für ein Werbemailing gekauft haben),

➔ bei Übermittlung der personenbezogenen Daten an ein Drittland oder eine internationale Organisation; Angaben zur Garantie gemäß Artikel 46 DSGVO. Das ist für Vereine in der Regel aber eher uninteressant.

Das bedeutet das neue Zugriffsrecht

Ergänzend zu den Auskunftspflichten besteht neu jetzt ein Zugriffsrecht (Art. 15 Abs. 3 DSGVO). Im Klartext bedeutet das, dass Sie den Betroffenen auf Verlangen eine Kopie der gespeicherten Daten zur Verfügung stellen müssen.

Diese Regelung ist im Prinzip noch nicht weiter dramatisch. Doch die Datenschutzgrundverordnung verlangt auch, dass Sie nach Möglichkeit den Fernzugang (via Internet) zu einem sicheren System bereitstellen, der dem Betroffenen direkten Zugang zu seinen personenbezogenen Daten ermöglicht.

Beispiel:

Der TSV Musterhausen gibt seinen Mitgliedern über ein Online-Portal die Möglichkeit, ihre persönlichen Mitgliedsdaten einzusehen und zu pflegen. Über entsprechende Passwörter ist sichergestellt, dass jedes Mitglied nur Zugriff auf seine Daten hat.

Berichtigungspflicht

Aus Artikel 16 des GVO ergibt sich ein Berichtigungsrecht. Sind Daten falsch, dürfen Betroffene von Ihrem Verein die unverzügliche Berichtigung verlangen.

Recht auf Löschung

Nach wie vor besteht das Recht auf Löschung dann, wenn die Speicherung der Daten unzulässig war. Das Gleiche gilt,

In diesen Fällen müssen Daten gelöscht werden

- ➔ wenn Daten für die Zwecke, für die sie erhoben wurden, nicht mehr benötigt werden,
- ➔ wenn die für die Datenverarbeitung notwendige Einwilligung widerrufen wurde,
- ➔ wenn ein Widerruf gemäß Artikel 21 (siehe oben) vorliegt,
- ➔ wenn die personenbezogenen Daten aufgrund einer gesetzlichen Verpflichtung zu löschen sind.

Überprüfen Sie Ihre Vorbereitungen mit folgenden Kontrollfragen:

- ➔ Haben Sie geregelt (und dokumentiert) wie verfahren wird, wenn jemand verlangt, dass seine Daten gelöscht werden?
- ➔ Wie stellen Sie ggf. sicher, dass die Daten wirklich aus allen Systemen gelöscht werden?
- ➔ Wie stellen Sie gff. sicher, dass Dritte, denen Sie die Daten weitergegeben haben, über die Löschung informiert werden?

Benachrichtigungspflichten bei Datenpannen

Weiter muss Ihr Verein Vorkehrungen treffen, damit im Falle einer Datenschutzverletzung (z. B. Klau von Mitgliedsausweisen oder -daten) die betroffenen Mitglieder unverzüglich innerhalb von 72 Stunden informiert werden können. Eine Datenschutzverletzung liegt vor, wenn

- ➔ es unbeabsichtigt oder unrechtmäßig
- ➔ zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von persönlichen Daten kommt oder

➔ es unbefugten Zugang zu personenbezogenen Daten gegeben hat.

Dabei kommt es nicht drauf an, ob die Datenschutzverletzung absichtlich oder versehentlich erfolgt ist.

TIPP:

Sobald es zu einer Datenpanne gekommen ist, müssen Sie abschätzen, ob Risiken für natürliche Personen wahrscheinlich sind.

➔ Dazu gehören Diskriminierung, Identitätsdiebstahl oder ein finanzieller Verlust. Dokumentieren Sie Ihre Risikoabwägung.

Information des Betroffenen

Betroffene müssen Sie über die Datenpanne informieren, wenn diese mit einem „hohen Risiko“ für ihn verbunden ist. Erforderlich ist eine unverzügliche und klare Benachrichtigung in einfacher Sprache. Machen Sie dabei mindestens Angaben zu den folgenden Punkten:

1. Nennen Sie Namen und Kontaktdaten Ihres Datenschutzbeauftragten (wenn ein solcher erforderlich ist; Genaueres dazu erfahren Sie unten).
2. Geben Sie eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes der Daten (z. B.: „Es ist nicht ausgeschlossen, dass Dritte die Informationen über Ihre Kontoverbindung nutzen, um sie als Zahlungsmittel bei Online-Käufen einzusetzen …“).
3. Beschreiben Sie die von Ihnen ergriffenen oder vorgeschlagenen Maßnahmen zur Reduzierung des Risikos und zur Behebung des Schadens.

Nur in bestimmten Ausnahmefällen können Sie auf diese Information verzichten, nämlich wenn:

- ➔ Sie technische und organisatorische Sicherheitsvorkehrungen angewandt haben, die personenbezogene Daten für Dritte unzugänglich machen, die öffentlich gewordenen Daten also beispielsweise verschlüsselt sind, oder
- ➔ Sie sichergestellt haben, dass das hohe Risiko für die Rechte und Freiheiten der Betroffenen aller Wahrscheinlichkeit nach nicht mehr besteht, oder
- ➔ die Information mit einem unverhältnismäßig hohen Aufwand verbunden wäre (dann ist allerdings eine öffentliche Bekanntmachung oder ähnliche Maßnahme notwendig, mit der die Betroffenen informiert werden).

Information der Aufsichtsbehörde

Neben den Betroffenen müssen Sie den Datenschutzbeauftragten Ihres Bundeslandes informieren, wenn es zu Datenpannen kommt.

Auch diese Information sollte unverzüglich möglichst innerhalb von 72 Stunden, nachdem Ihnen der Vorfall bekannt geworden ist, erfolgen.

In Artikel 33 DSGVO ist geregelt, was Sie dem Datenschutzbeauftragten alles mitteilen müssen:

- ➔ Was ist passiert und wie viele Personen und Datensätze sind ungefähr betroffen?
- ➔ Welche Folgen hat die Verletzung der personenbezogenen Daten?
- ➔ Was haben Sie getan, um die Folgen zur Beseitigung oder abzumildern.

Falls in Ihrem Verein ein Datenschutzbeauftragter erforderlich ist (siehe unten), müssen Sie der Aufsichtsbehörde auch dessen Namen und Kontaktdaten übermitteln.

Wichtig:

Dokumentieren Sie unbedingt die Datenpanne, ihre Auswirkungen sowie die von Ihnen ergriffenen Maßnahmen umfassend.

Tipp:

Legen Sie bereits jetzt einen Kommunikationsplan und die entsprechenden Verantwortlichkeiten fest. Damit sparen Sie sich in der sowieso stressbelasteten Situation einer Datenschutzpanne unnötigen Ärger und tragen zur Entspannung bei.

Brauchen Sie einen Datenschutzbeauftragten?

Sind in Ihren Verein in der Regel mind. zehn Personen mit der automatisierten Verarbeitung von personenbezogener Daten beschäftigt, dann müssen Sie unbedingt einen Datenschutzbeauftragten bestellen (§ 38 BDSG-neu).

Dabei spielt es keine Rolle, ob diese Personen hauptamtlich oder ehrenamtlich Tätige sind.

Maßnahmen der Datensicherheit/ Datenschutzes

Artikel 24 DSGVO schreibt vor, dass Sie unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung von Daten sowie der Möglichkeit und Schwere von Risiken geeignete technische und organisatorische Maßnahmen treffen müssen, um diese zu vermeiden. Außerdem sollen Sie den Nachweis dafür bringen können, dass die Datenverarbeitung gemäß der DSGVO erfolgt. Im Prinzip läuft es darauf hinaus, dass Sie ein Datenschutzkonzept formulieren und vorhalten müssen.

Checkliste: So bereiten Sie sich auf die neue DSGVO vor

Die neue Datenschutzgrundverordnung enthält noch zahlreiche weitere Vorgaben, die für Ihren Verein je nach konkreter Ausgestaltung des Vereins wichtig sind. Nutzen Sie die verbleibenden Monate bis zum 25. Mai 2018, um sich mit den neuen Bestimmungen vertraut zu machen und Ihren Verein insoweit fit zu machen. Denn es gibt vorher einiges zu bedenken und zu erledigen. Beginnen Sie dazu mit den Maßnahmen aus der folgenden Checkliste.

Checkliste: Vorbereitung auf die Einführung der DSGVO

Planen Sie für die nächsten Monate bis zum Stichtag Ende Mai 2018 zeitliche, personelle und finanzielle Ressourcen zur Vorbereitung auf die DSGVO ein.	
Nutzen Sie bereits jetzt Weiterbildungsangebote, z. B. der Dachverbände, um die verantwortlichen Vorstandsmitglieder fit zu machen.	
Analysieren Sie, wo in Ihrem Verein mit personenbezogenen Daten von Mitgliedern, Interessenten und Mitarbeitern umgegangen wird. Klären Sie dabei: Um welche Daten handelt es sich? Wie werden diese erhoben, gespeichert und verarbeitet? Wer darf darauf zugreifen und wie ist der Zugriff geschützt?	
Die DSGVO stellt noch mehr als bisher das BDSG darauf ab, dass nur erforderliche Daten verarbeitet werden. Überprüfen Sie Daten auf Erforderlichkeit und löschen Sie ggf. nicht erforderliche.	
Entwickeln Sie Sicherheitsmaßnahmen, um jeden unberechtigten Zugriff und jeden Datenverlust zu verhindern.	
Wenn Sie Leistungen an externe Partner ausgegliedert haben, bestehen Sie darauf, dass ihnen entsprechende Sicherheitskonzepte vorgelegt werden. Diese sollten regelmäßig geprüft werden.	
Überprüfen Sie, ob Einwilligungen zur Datenverarbeitung frei von vorausgefüllten Kästchen und stillschweigenden Zustimmungen sind. Ggf. sind diese anzupassen.	
Stellen Sie sicher, dass Einwilligungen hinreichend deutlich machen, welche konkrete Datenverarbeitung der Nutzer zu welchem Zweck einwilligt.	
Stellen Sie sicher, dass Einwilligungen zur Datenverarbeitung mit Datum versehen und dokumentiert sind.	
Regeln Sie, wie in Ihrem Verein mit den acht wesentlichen Datenschutzprinzipien (siehe oben) umgegangen wird.	

Impressum

Verlag für die Deutsche Wirtschaft AG
Theodor-Heuss-Straße 2-4
D-53177 Bonn
Großkundenpostleitzahl: D-53095 Bonn

Tel.: 0228 - 9 55 01 0 (Kundendienst)
Fax: 0228 - 36 96 480

USt.-ID: DE 812639372
Amtsgericht Bonn, HRB 8165

Internet: www.wirtschaftswissen.de
E-Mail: kundendienst@vnr.de

Vorstand: Richard Rentrop

Bildnachweis: www.fotolia.com
Autor: Rechtsanwalt und Vereinsexperte Heiko Klage